# 如何確定特定Snort例項處理的流量

#### 目錄

簡介

必要條件

需求

採用元件

設定

組態

驗證

疑難排解

## 簡介

本文說明如何確定特定snort例項正在處理的流量。在對特定Snort例項上的CPU使用率較高進行故障排除時,此詳細資訊非常有用。

### 必要條件

#### 需求

思科建議您瞭解以下主題:

• Firepower技術知識

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Firepower管理中心6.X及更高版本
- 適用於所有受管裝置,包括Firepower威脅防禦、Firepower模組和Firepower感測器本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設)的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### 設定

#### 組態

以管理許可權登入到Firepower管理中心。

#### 登入成功後,導覽至Analysis > Search,如下圖所示:

		telligence		Deploy
ext Explorer Connect	ions ▼ Intrusions ▼ Files ▼ Hosts	S ▼ Users ▼ Vulnerabilities ▼ Corre	elation ▼ Custom ▼ Lookup ▼	Search
	Connection Events \$	(unnamed search)	Private	Save Save As New Search
	Sections	Device		
	General Information	Device*		device1.example.com, *.example.com, 192.1
	Networking	Ingress Interface		s1p1
	Geolocation	Egress Interface		s1p1
	Device	Ingress / Egress Interface		s1p1
	SSL	Snort Instance ID		
	Application			1
	URL	SSL		
	Netflow	SSL		yes, no
	QoS	SSL Status		Decrypt, Success, Block, Failure
	QUS	SSL Flow Error		Success, NS_INTERNAL_ERROR
		SSL Actual Action		Decrypt, Block
	+ New Search	SSL Expected Action		Decrypt, Block
	Predefined Searches	SSL Failure Reason		Success, Failure
	Malicious URLs	SSL Certificate Status		Revoked, Self Signed, "Self Signed, Revoked
		SSL Version		SSLv3.0, TLS
	Possible Database Access	SSL Cipher Suite		SSL2, AES
	Risky Applications with Low Business Relevance	SSL Policy		My SSL Policy
	Standard HTTP	SSL Rule		My SSL Rule
	Standard Mail	SSL Session ID		
	Standard SSL	SSL Ticket ID		
		SSL Flow Flags		FULL_HANDSHAKE
		SSL Flow Messages		CLIENT_FINISHED
		SSL Certificate Fingerprint		C1 37 4D 95 55 19 DD 80 AF 02 F8 6D 05 E
		SSL Subject Common Name		cisco.com

確保從下拉選單中選擇**Connection Events**表,然後從部分中選擇**Device**。為「Device(裝置)」欄位和「Snort Instance ID(Snort例項ID)」輸入值(0到N,Snort例項的數量取決於受管裝置),如下圖所示:



輸入值後,按一下Search,結果將是由特定snort例項觸發的連線事件。

附註:如果受管裝置是Firepower威脅防禦,則可以使用FTD CLISH模式確定snort例項。

**附註**:如果受管裝置是Firepower模組或Firepower感測器,您可以使用專家模式和基於 Linux的**top**命令確定snort例項。

admin@firepower:~\$ top

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND 5247 root 20 0 15248 1272 932 S 0 0.0 0:03.05 top 5264 root 1 -19 1685m 461m 17m S 0 2.9 1:05.26 snort

### 驗證

目前沒有適用於此組態的驗證程序。

# 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。